TUNIS BUSINESS SCHOOL
UNIVERSITY OF TUNIS

CertifyPro: ISO Certification Simulation Platform

A Project by:

Mahdi Messai

Contents

1 Introduction

1.1 Project Overview

The CertifyPro ISO Certification Simulation Platform is a backend system designed to simulate and streamline ISO certification processes. It provides an environment for organizations and certification bodies to understand and manage certification processes.

The core objective is to build a robust, and secure backend supporting key ISO certification functionalities:

- **Secure Authentication & Authorization**: Employ JWT for secure API endpoint protection and data confidentiality.
- **Role-Based Access Control**: Implement distinct user roles (admin, managers, employees, auditors, guests) with tailored permissions.
- **Organization & Certification Body Management**: Enable creation, approval, and member management for organizations seeking certification and certification bodies providing it.
- **Audit Simulation**: Facilitate audit requests, scheduling, tracking, and status updates between organizations and certification bodies.
- **Certification Management**: Manage ISO certification issuance, tracking, status, and generate certificates in PDF format upon successful audits.
- **ISO Standards Database & AI Chat**: Integrate a searchable ISO standards database and an AI-powered chat (Gemini API) for intelligent ISO information access.
- **Automated Communication**: Streamline notifications via email for account actions, invitations, audit updates, and certifications.

1.2 Target Users and Use Cases

CertifyPro serves diverse users within the ISO certification ecosystem:

- **Organizations Seeking Certification**: Request audits, manage profiles/members, track progress, access ISO standards info, and use AI chat for guidance.
- **Certification Bodies**: Manage audit requests, schedule audits, issue/revoke certifications, manage profiles/members, and access ISO standards data.

CertifyPro streamlines and simulates the ISO certification lifecycle, providing a centralized, efficient, and informative platform for all stakeholders.

2 System Architecture and Design

2.1 Overall Architecture

The CertifyPro platform is built upon a well-established three-tier architecture, ensuring a clear separation of concerns and promoting scalability and maintainability. This architecture is complemented by the modular structure of the Flask application, utilizing Blueprints to organize functionalities into distinct components.

2.1.1 Three-Tier Architecture (Presentation, Application, Data)

The three-tier architecture logically divides the system into the following layers:

- **Presentation Tier (Frontend):** This layer is responsible for user interaction and display. In the context of CertifyPro, this is envisioned as a separate frontend application (using React) that interacts with the backend API. This report primarily focuses on the backend system, and thus, the frontend tier will only be briefly discussed later in the document.
- **Application Tier (Backend - Flask Application):** This is the core of the CertifyPro platform. It handles business logic, data processing, security, and API endpoints. The application tier receives requests from the presentation tier, processes them using the defined business rules, interacts with the data tier, and returns responses back to the presentation tier.
- **Data Tier (Databases):** This layer is responsible for data storage and retrieval. CertifyPro employs a dual-database strategy:
  - **PostgreSQL:** A relational database managed using SQLAlchemy ORM, used for structured data such as user accounts, organization details, certification bodies, audit records, certifications, requests, and invitations.
  - **MongoDB:** A NoSQL document database accessed via PyMongo, used for storing ISO standard documents. MongoDB is chosen for its flexible schema.

This separation into tiers allows for independent development and maintenance of each layer. Changes in one tier do not impact other tiers.

2.1.2 Database Models

CertifyPro utilizes a set of database models representing core entities such as Users, Organizations, Certification Bodies, Audits, Audit Requests, and Certifications. The following class diagram visually illustrates the relationships and key attributes of these core database models.

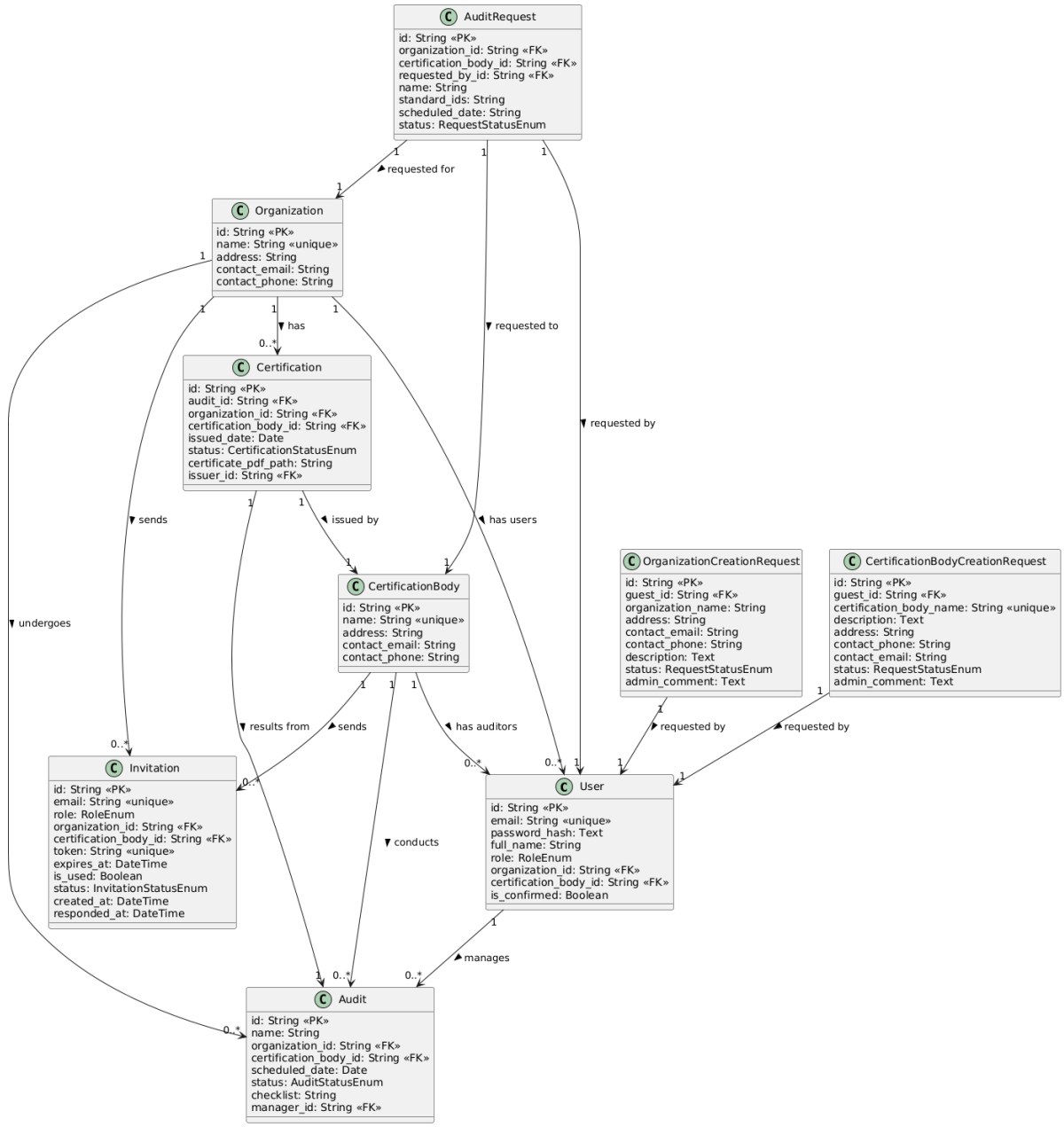

Figure 1: CertifyPro Flask Application Blueprint Structure

3 Core Functionalities and Features

3.1 User Authentication and Authorization

Registration, Login, Logout Users can register either via invitation from organizations/certification bodies or as guest users (requiring email verification). Registered users can log in with email and password to obtain secure access. Logout functionality revokes access tokens. Password reset workflows are also supported via email.

Role-Based Access Control (RBAC) The platform implements distinct roles: Admin, Manager (Organization/Certification Body), Employee, Auditor, and Guest. Access to functionalities is strictly controlled based on these roles. Administrators have the highest privileges, followed by Managers, while Employees, Auditors, and Guests have progressively limited access.

Token Management (JWT) Secure session management is handled using JWTs. Upon login, users receive a JWT for authenticated access, ensuring stateless and scalable authorization. Tokens have limited lifespans and can be revoked for logout, enhancing security.

3.2 Organization and Certification Body Management

Creation Request Workflows Guest users can request to create new organizations or certification bodies. Administrators review and approve or reject these requests. Upon approval, the requesting guest becomes a Manager of the newly created entity.

Invitation System for Members Managers can invite users to join their organizations or certification bodies with specific roles (Employee, Auditor, Manager). Invitations are sent via email with secure tokens for acceptance. Managers can also revoke pending invitations.

Member Management (Adding, Removing, Viewing) Managers can view lists of members within their organizations or certification bodies. They also have the ability to remove members, effectively demoting them to guest users and removing their organizational affiliation.

3.3 Audit Management

Audit Request Process Organization Managers can request audits from Certification Bodies. Certification Body Managers are notified of these requests and can approve or reject them. Upon approval, an audit is scheduled. Certification Body Managers can also directly create audits for organizations without a prior request.

Audit Scheduling and Status Updates Audits are scheduled with defined dates and statuses (Scheduled, In Progress, Completed). Certification Body Managers can update the status of audits to reflect their progression.

Audit Retrieval and Details Authorized users (depending on role and affiliation) can retrieve lists of audits and view detailed information about specific audits, including status, scheduled date, and associated organizations/certification bodies.

3.4 Certification Management

Certification Issuance based on Audits Certification Body Managers can issue certifications upon successful completion of audits. The system verifies audit completion before allowing certification issuance. Issuance automatically generates a PDF certificate.

Certificate Generation and Download The platform automatically generates PDF certificates upon certification issuance. Authorized users can download these certificates.

Certification Status and Retrieval Users can retrieve lists of certifications relevant to their organizations or certification bodies. The system tracks certification status (e.g., Issued, Revoked).

3.5 ISO Standards Information Retrieval

Searching and Filtering ISO Standards Users can search and filter ISO standards based on keywords, categories, and other criteria. The system allows for efficient retrieval of relevant standards from the database.

AI-Powered Chat for ISO Standard Queries Users can utilize an AI-powered chat interface to ask questions about ISO standards in natural language and receive business-focused and actionable answers, powered by the Gemini API.

3.6 Admin Panel and User Management

Admin User Role and Permissions Administrators possess the highest level of access, enabling them to manage users, approve creation requests, and perform system-level tasks.

User Listing and Overview Administrators can access a list of all users within the platform to oversee user accounts and roles across organizations and certification bodies.

3.7 Blueprints and API endpoints

The CertifyPro backend exposes a RESTful API, with endpoints logically grouped under each Blueprint's URL prefix.

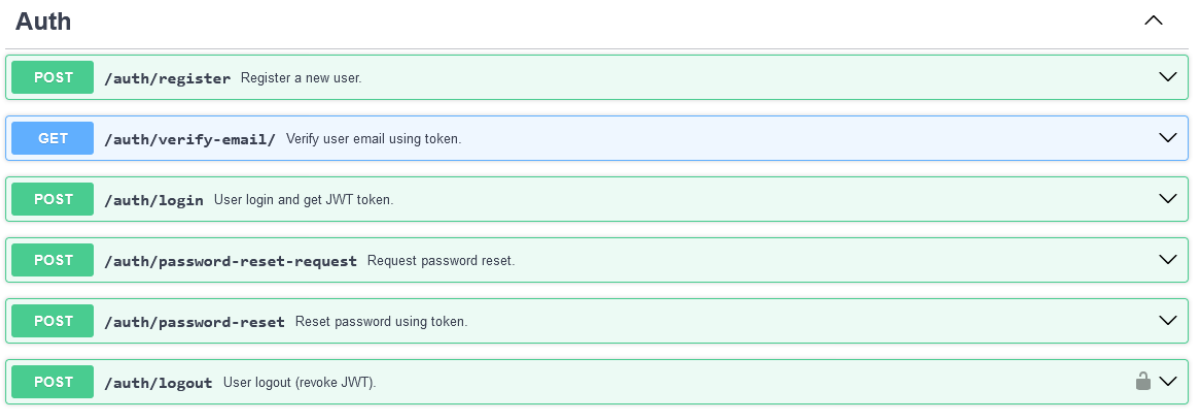

Figure 2: Auth Blueprint

Auth Blueprint: Handles user authentication, registration, login, logout, password reset, and email verification.

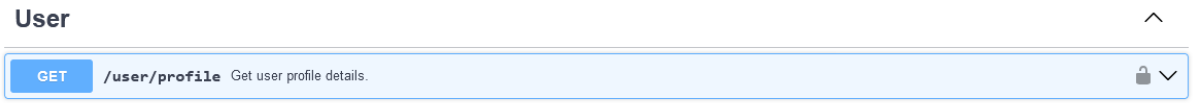

Figure 3: User Blueprint

User Blueprint: Manages user profile retrieval.

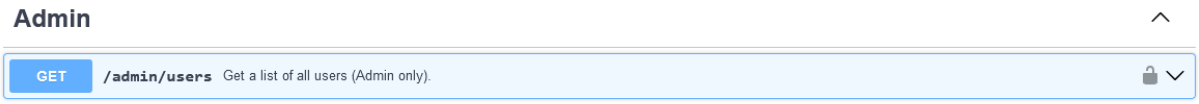

Figure 4: Admin Blueprint

Admin Blueprint: Provides administrative functionalities, such as user listing.

Figure 5: Organization Blueprint

Organization Blueprint: Manages organization creation requests, organization invitations, and organization member management.

Figure 6: CertificationBody Blueprint

CertificationBody Blueprint: Manages certification body creation requests, certification body invitations, and certification body member management.

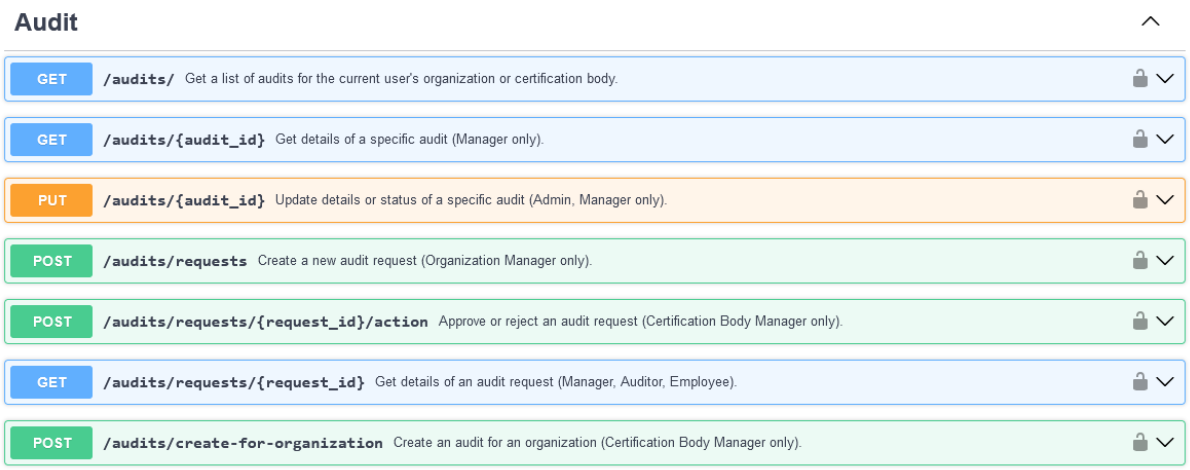

Figure 7: Audit Blueprint

Audit Blueprint: Handles audit requests, audit creation, and audit status updates.

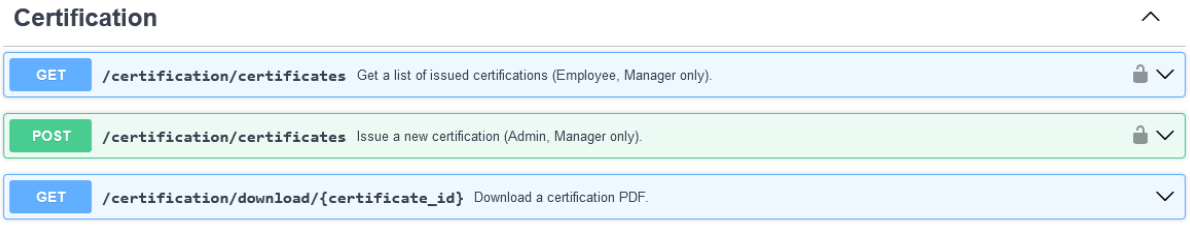

Figure 8: Certification Blueprint

Certification Blueprint: Manages certification issuance and certificate downloads.

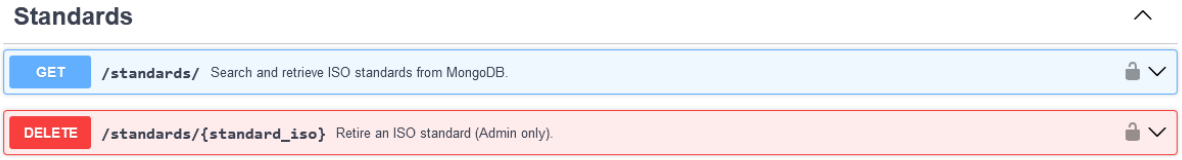

Figure 9: Standards Blueprint

Standards Blueprint: Provides API endpoints for searching and retrieving ISO standard data from MongoDB.

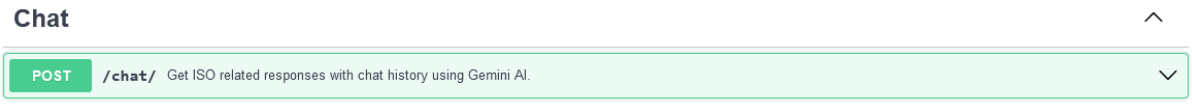

Figure 10: Chat Blueprint

Chat Blueprint: Integrates the Gemini AI API for ISO-related chat functionality.

3.8 Technology Stack

Initially, to populate the MongoDB database with a comprehensive dataset of ISO standards, we employed **Scrapy**, a web scraping framework. A Scrapy spider was developed to crawl the ISO website,

extract data points for each standard – including ISO number, category, subcategory, description, and other metadata – and store this information as documents within MongoDB. This data ingestion process ensures that the platform provides users with a rich and searchable repository of ISO standards from the outset.

The key components of the technology stack are summarized below:

- **Backend Framework: Flask**
- **Relational Database: PostgreSQL**
- **Document Database: MongoDB**
- **Authentication & Authorization: Flask-JWT-Extended**
  - JWT-based token authentication for secure API access.
  - Role-Based Access Control (RBAC) for endpoint protection.
- **Email Services: Flask-Mail**
  - Simplifies email sending from Flask applications.
  - Automated emails for account confirmation, password reset, invitations, and notifications.
- **AI Chat Integration: Gemini API (Google Generative AI)**
  - Provides intelligent, business-focused ISO information via chat.
  - Leverages 'gemini-exp-1206' model for relevant responses.
  - Manages chat history for contextual conversations.
- **Frontend Framework: React + TailwindCSS**